Australian Government

Australian Institute of Criminology

Trends & issues in crime and criminal justice

ISSN 0817-8542

No. 569 March 2019

Abstract | Identity crime and misuse cost the Australian economy an estimated $2.65b in 2015–16 (Jorna & Smith 2018). Considerable effort has been devoted to finding secure ways to verify individuals' identity and to secure their personal information.

Biometrics is the fastest developing technological solution. It makes use of people's unique biological characteristics to identify them when dealing with government and business.

Since 2013, the Australian Institute of Criminology has conducted online surveys to gain a greater understanding of identity crime and misuse in Australia. These surveys have asked about respondents' experience of identity crime and also their willingness to use biometric technologies to safeguard their personal information.

This paper presents the results of the latest survey, conducted in 2017, which indicated generally high levels of previous exposure to biometrics and increasing willingness to use biometric technologies in the future.

Use and acceptance of biometric technologies in 2017

Russell G Smith, Alexandra Gannoni and Susan Goldsmid

Introduction

As part of the Australian Government's National Identity Security Strategy (AGD 2013), a sample of Australians were surveyed about their experience of identity crime and misuse and how they responded to the problem. In addition to finding out how prevalent misuse of personal information is, the surveys asked respondents to indicate how willing they were to use various biometric technologies to protect their personal information (Emami, Brown & Smith 2016).

This paper presents the findings of the surveys conducted in 2014, 2016 and 2017 that relate specifically to previous use of biometrics and willingness to use biometrics in the future. It provides updated information on the findings of the 2014 survey, which was the first to assess the willingness of Australian victims of identity crime to use biometrics to enhance the security of their personal information (Emami, Brown & Smith 2016). The other more general findings of the identity crime and misuse surveys have been published elsewhere (Goldsmid, Gannoni & Smith 2018; Smith, Brown & Harris-Hogan 2015; Smith & Hutchings 2014; Smith & Jorna 2018).

The place of biometrics in identity security

Biometric technologies use an individual's unique physiological or behavioural attributes as a means of identification. They include fingerprint matching, signature analysis, or recognition of a person's retina, iris, face or voice. Facial recognition is now considered to be the dominant biometric technology globally and the one most likely to increase in use over the next few years. The findings of the Biometrics Institute's annual surveys of members since 2010 have shown that facial recognition has continued to grow in importance. These surveys are conducted annually and are sent by the Biometrics Institute to its 6,000 individual members and other stakeholders worldwide. In June 2018, 310 individuals responded to the survey, representing suppliers of biometrics (48%), users (38%) and other interested organisations and industries (14%; Biometrics Institute 2018).

The 2018 survey found that 47 percent of respondents considered facial recognition to be the biometric technology most likely to be on the increase over the next few years (Biometrics Institute 2018). This was followed by iris recognition (8%), fingerprint recognition (7%) and voice recognition (6%). A further 19 percent of survey respondents considered that multi-modal approaches that combine various biometrics would be most likely to increase over the next few years (Biometrics Institute 2018).

Biometric technologies are currently used by a range of organisations in Australia to verify the identities of the people with whom they deal. For example, the Department of Home Affairs collects biometric information including fingerprints and facial images from offshore visa applicants, onshore protection visa applicants, immigration detainees, and certain categories of airline passengers (Department of Home Affairs 2018).

Australian airports have facial recognition capabilities, known as SmartGates, that enable travellers with ePassports from Australia, New Zealand, the United Kingdom, Switzerland, Singapore and the United States to process themselves rather than undergoing the customs and immigration checks that are usually conducted by Australian Border Force officers (Department of Home Affairs 2018). Standards for the interoperability of biometric systems have also been developed to promote the effective operation of biometric systems between various government agencies (AGD 2012).

In addition, biometrics have been introduced to verify an individual's identity in a range of other settings. For example, a number of financial institutions are considering using biometric technologies such as fingerprint recognition for payment card authentication and for mobile banking services instead of passwords and PINs (Saarinen 2017). Iris recognition has also been used for cardless ATM transactions (Kim 2015). In Australia, the National Australia Bank and Microsoft have collaborated to design a proof of concept ATM using biometrics, cloud and artificial intelligence technologies; this would enable customers to withdraw cash from ATMs using facial recognition technology and a PIN (Planet Biometrics 2018).

Respondents to the Biometrics Institute's survey in 2018 indicated that the most significant development in the use of biometrics during the last 12 months related to border control/security, accounting for 20 percent of responses. This was followed by online identity verification (12%), large-scale national identity deployments (9%), financial services (8%) and mobile payments/m-commerce, device access and surveillance (these last three types accounting for 7 percent each). Respondents also indicated that over the next five years the most important developments would occur in relation to online identity verification (20%), large-scale national identity deployments (11%) and border control/security (11%; Biometrics Institute 2018).

Advantages and challenges of biometrics

There are various reasons why biometric solutions to identity crime have developed so strongly in recent years. For users, card-free biometric systems are easy to use and efficient when engaging with government and business, particularly when conducting financial transactions online. Conventional user-authentication systems that rely on knowledge-based identifiers such as passwords and PINs are impractical when individuals are required to identify themselves for multiple purposes and on multiple occasions, particularly online. This has led to users adopting workarounds such as keeping passwords in electronic files, which can easily be compromised. Worse still is the practice of writing passwords and PINs on paper notes, which not only can be read by others, but can make one ineligible for compensation if fraud occurs. Devices for entering PINs have created many opportunities for scanning and skimming—crimes that are difficult and costly to resolve. Having a biological identifier overcomes these physical and practical limitations.

From an industry and government business perspective, reducing the risk of identity crime leads to less card and transaction fraud, avoids theft and compromise of PINs, and reduces the costs associated with dealing with the consequences of fraud and lost or stolen cards for government and business enterprises. Biometrics also have faster processing times than other technologies and they can be easily integrated with other authentication processes.

There are, however, a number of challenges associated with using biometrics to identify individuals (Smith, Mann & Urbas 2018; Smith 2007). Foremost among these are the risks of infringement of privacy and misuse of biometrics for unauthorised tracking of business transactions and locations of individuals. There are also concerns that governments may exceed their authority by using biometrics to identify individuals for data matching, identification and surveillance purposes (United States Government Accountability Office 2002). These risks also affect conventional user authentication processes, although the efficiency of biometric technologies makes function creep more problematic than in the case of conventional authentication systems (Smith, Mann & Urbas 2018; Smith 2006).

Although biometric identification minimises the risk of most types of identity crime, opportunities for fraud still exist when individuals first enrol with government organisations and businesses. Once an individual has registered legitimately using false or fabricated information, it is difficult to detect the fraud, challenge the enrolment and locate the individual responsible. Biometric systems also have high implementation costs associated with terminal upgrades and enrolment procedures as well as high costs of public education prior to roll-out. There are also risks of biometric data being compromised or stolen and administrative problems associated with reinstating compromised biometrics (Smith 2006).

Various crime displacement risks have also been identified, including the possibility of individuals being compelled under threat of violence to present their biometric identifiers at secure buildings or terminals to allow access, or being kidnapped and forced to withdraw funds from ATMs or banks (Rowe et al. 2013). Finally, there is the problem of end-user resistance to the use of biometrics due to health, security or privacy concerns. It is this final challenge that forms the subject of the present research.

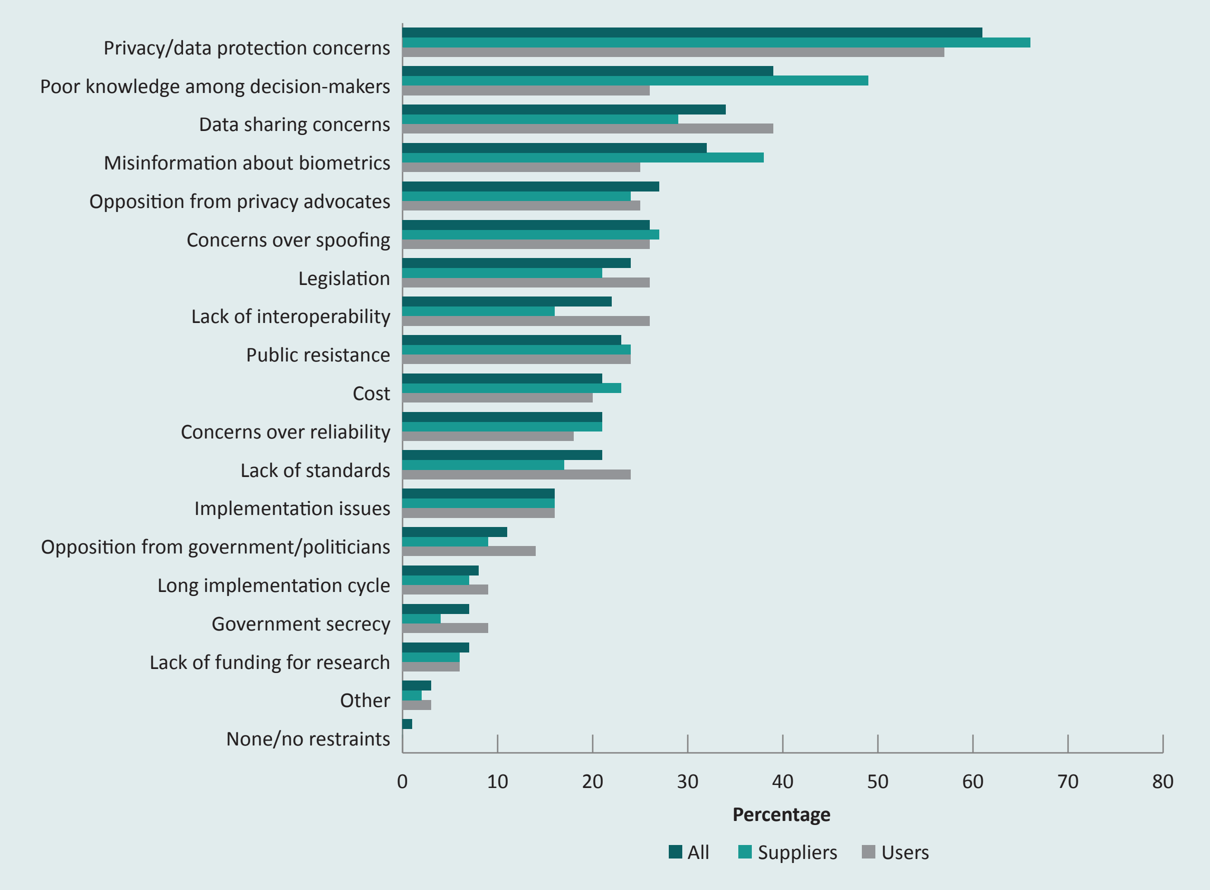
Attitudes towards biometrics

Emami, Brown and Smith (2016) reviewed prior research that investigated people's willingness to use biometric technologies to minimise the risks of identity crime and misuse, citing the observation of the United Kingdom Biometrics Working Group (2001: 7) that 'user attitude can make or break the implementation of a biometric system'.

Research on the attitudes of members of the Australian public towards the use of biometric technologies has found that while many Australians are comfortable with these technologies being used for security purposes and to verify identity in order to access government services, there is much greater apprehension around the use of biometrics for marketing purposes, accessing public transport or enrolling in educational courses (Emami, Brown & Smith 2016). These latter situations are thought to entail increased risks of theft or fraud that many users are unwilling to take.

More recently, the Biometrics Institute survey for 2018 asked its 310 respondents to identify the top four factors that restrain the biometrics market. Figure 1 shows the results for all 279 respondents who answered this question as well as for the 126 suppliers and 103 user respondents to this question. Privacy/data protection concerns continued to be rated as the greatest market restraint, with well over half (61%) feeling they restrained the market in 2018 (an increase of 4 percentage points on 2017). Both suppliers and users selected a similar number of restraints on average and both viewed privacy/data protection concerns as the main factor restraining the market. Concerns about data sharing, legislation and public resistance to biometrics also increased between 2017 and 2018, while opposition from privacy advocates declined in perceived importance by four percentage points.

Figure 1: Market restraints for biometrics, 2018



Source: Biometrics Institute (2018: 19–20)

Other research has explored the reasons individual users are willing or unwilling to use biometric technologies, with the service provider (public or private sector) being one important factor in establishing trust. For example, Australians are reasonably comfortable with using biometrics for airport security and passenger processing (Unisys 2014). Border control/security was also the area identified by respondents to the 2018 Biometrics Institute survey as having the greatest industry development over the preceding 12 months. This also confirms the finding that facial recognition (which is almost exclusively the biometric favoured in airports) is the technology that respondents to the Biometrics Institute's 2018 survey considered to be most likely to increase in the years ahead—rated highest by 47 percent of respondents in 2018 and 38 percent in 2017 (Biometrics Institute 2018).

Methodology

In July 2017, a questionnaire comprising 37 main questions was administered online to a research panel of Australians drawn from all states and territories. A sampling frame of more than 300,000 individuals was provided by the market research company i-Link Research Solutions, which also hosted the online questionnaire and provided raw, de-identified data for the Australian Institute of Criminology (AIC) to analyse.

Sampling was completed once a quota of 10,000 respondents had been satisfied. No other quotas were employed as the sample was sufficiently large to ensure good representation from urban and regional areas across Australia.

Data were weighted by age and gender to represent the spread of the population in Australia. Australian Bureau of Statistics data from the 2016 Census were used to develop the weighting matrix for the sample data. The Census data did not provide population data for people who listed their gender as ‘indeterminate/intersex or unspecified’. Accordingly, responses from 38 respondents who fell within this group were excluded as weighting could not be undertaken using available data. A small number of respondents who did not specify their age were also excluded from the analysis (n=29). This resulted in a useable sample size of 9,947 respondents.

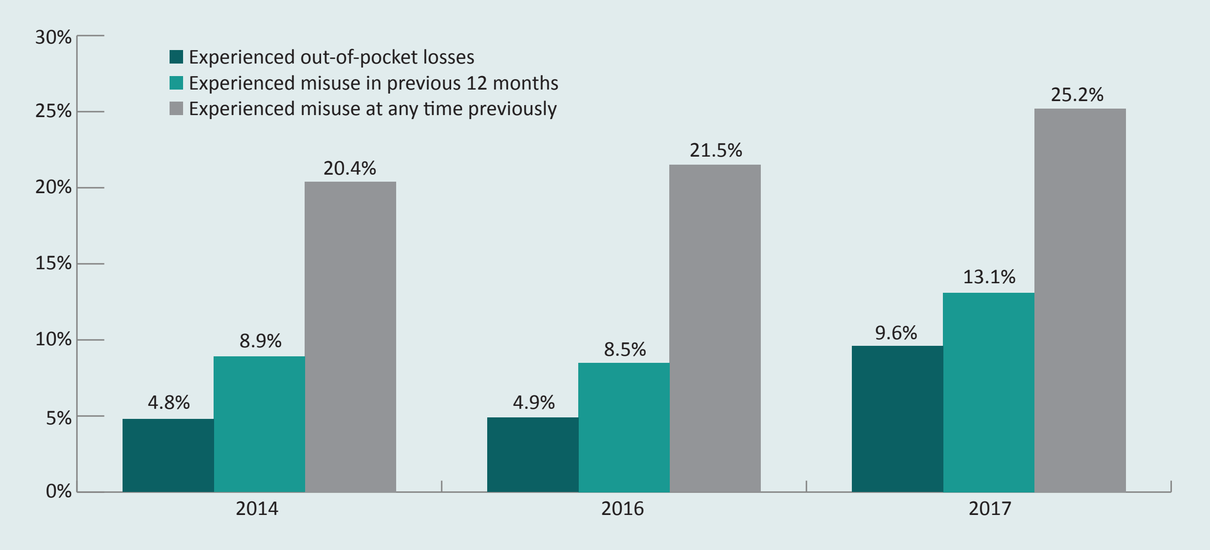
The methodology employed was generally the same as that used in the Identity Crime and Misuse in Australia surveys conducted by the AIC in 2014 (Smith, Brown & Harris-Hogan 2015) and 2016 (Smith & Jorna 2018). Differences included an increase in sample size from 5,000 in 2014 to 9,956 in 2016 and 9,947 in 2017, and the fact that the questions on biometrics were asked of all respondents, not only those who had reported misuse in the previous 12 months, as in the 2014 survey. In both 2016 and 2017, all respondents answered questions about their willingness to use biometrics. Further information about the sampling and research methodology are contained in the principal report (Goldsmid, Gannoni & Smith 2018).

Findings

Victimisation

The results of the 2017 survey showed that 13 percent of respondents reported having had their personal information misused in the preceding 12 months, and 25 percent of respondents reported misuse of their personal information at some time during their life (Goldsmid, Gannoni & Smith 2018). There were significant increases in those reporting lifetime misuse of personal information, misuse over the preceding 12 months and out-of-pocket losses between the surveys conducted in 2016 and 2017 (Figure 2).

Figure 2: Victimisation and out-of-pocket losses from misuse of personal information, 2014–17 (%)



Note: Statistically significant 3.7 percentage point rise in lifetime victimisation from 2016 to 2017 (N-1 $\chi^2(1)=38.06$, $p<0.001$) and a statistically significant increase from 2016 to 2017 in yearly victimisation (N-1 $\chi^2(1)=109.30$, $p<0.001$). 2014 data weighted by location and 2016 and 2017 data weighted by age and gender

Source: Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018; Goldsmid, Gannoni & Smith 2018

Previous use of security measures

Respondents were asked whether they had ever used specified security measures in the past—in any way, not just to prevent misuse of personal information. Consistent with previous surveys, the vast majority of respondents (93%) reported using at least one of the security technologies identified (see Table 1).

Passwords (91%) were the most common type of technology respondents had used in the past, as might be expected given their widespread use. This was followed by signatures (41%) and fingerprint recognition (35%). The least common type of technology respondents had used in the past was a computer chip implanted under the skin (3%). The response option 'computer chip implanted under the skin' was introduced in 2017 and so results cannot be compared with those of previous years—although the finding that three percent of respondents reported having used this in the past is surprising. This technology does, however, seem to be gaining ground, particularly in Sweden, where a state-owned railway company, SJ, has used scanned embedded chips to collect train fares from commuters. Thousands of Swedes have had microchips implanted as an alternative to using cards and PINs (Ma 2018).

Comparing 2016 and 2017 data, there were considerable increases in the use of fingerprint recognition (8 percentage points) and voice recognition (6 percentage points), and modest increases in the use of facial recognition (4 percentage points) and iris recognition (3 percentage points). These changes may be explained in part by the increasing adoption of biometrics in Apple and Android smartphones and the expansion of SmartGate facial recognition in airports (DIBP 2017). The 2014 survey found similar levels of prior use among victims of identity misuse, except for voice and iris recognition, which changed rank order slightly.

Table 1: Use of security measures in the past (%)

	2014	2016	2017	
Sample size (n)	5,000[a]	9,956	9,947	
Technology				**Percentage point change**
Passwords	88.3	90.8	90.8	0.0
Signatures[b]	–	41.8	41.4	–0.4
Fingerprint recognition	16.8	26.7	35.0	+8.3***
Voice recognition	5.6	11.5	17.9	+6.4***
Facial recognition	6.7	6.6	10.4	+3.8***
Iris recognition	5.8	1.9	5.2	+3.3***
Computer chip implanted under your skin[c]	–	–	2.6	–
Any technology[d]	94.8	92.8	93.3	+0.5
No technology	5.2	7.2	6.7	–0.5

***statistically significant at $p<0.001$

a: In 2014, only respondents who had experienced misuse of personal information in the preceding 12 months were asked about use of security measures

b: The 2014 survey did not ask about signatures

c: Included in 2017 identity crime survey only

d: Includes passwords, signatures, voice recognition, fingerprint recognition, facial recognition, iris recognition, and computer chip implanted under the skin (except for 2014, which excluded signatures and chip implants)

Note: Respondents could select multiple responses. 2014 data weighted by location; 2016 and 2017 data weighted by age and gender

Source: Identity crime surveys 2014, 2016, 2017 [AIC data file]

For the 2017 findings, chi-square tests were undertaken to identify whether previous use of biometrics was associated with demographic characteristics such as gender, age, Indigenous status, language spoken at home, income, whether or not they lived in a capital city and the number of hours spent per week on a computer. It should be noted, however, that all differences between specific categories were based on an analysis of the adjusted residuals. A chi-square analysis is used to test whether there is an association or relationship between variables. It examines the probability of the results occurring by chance. Further statistical tests were undertaken to determine whether previous use of the four biological biometrics (fingerprint, facial, iris and voice recognition), when grouped together, differed significantly among different demographic groups (Goldsmid, Gannoni & Smith 2018).

Where passwords were concerned, only one variable demonstrated a statistically significant difference. Those earning $180,000 or more were found to be significantly less likely (51%, n=7) than people with lower incomes to have used passwords in the past ($\chi^2(5, n=446)=12.51$, $p<0.05$). It is unclear why this was the case and future research is needed to examine this further. It is possible that individuals earning incomes of $180,000 or more rely on personal assistants and others to log on to networks on their behalf, and be responsible for user authentication in the workplace (Goldsmid, Gannoni & Smith 2018).

In the case of fingerprint recognition, 17 percent of respondents had previously used this technology. Previous use of fingerprint recognition technologies differed significantly by level of computer use ($\chi^2(6, n=442)=18.56, p<0.01$). Those using a computer for five hours per week or less were more likely to have used fingerprint recognition (46%, n=12), while those using a computer for 26 to 30 hours per week were less likely to have used this biometric (10%, n=6). One reason for this may be that those respondents who indicated that they used a computer for only five hours or less per week may rely on their smartphones or tablets instead of desktop computers. Given that a number of smartphones and tablets now use fingerprint recognition to verify identity, it is possible that this may explain why individuals who reported lower levels of computer use were more likely to have used fingerprint recognition compared to those who used a computer for between 26 and 30 hours per week (Goldsmid, Gannoni & Smith 2018).

Facial recognition (10%) and iris recognition (5%) had been used by a small number of respondents. In the case of facial recognition, this is somewhat surprising, as 14.6m passengers used SmartGates at Australian international airports in 2016–17 (DIBP 2017). SmartGates use facial recognition technology in conjunction with data contained in the ePassport chip to verify travellers' identities (DIBP 2017). It may be that those using SmartGate terminals did not realise that this was a form of facial recognition, or perhaps the 2017 survey respondents had not used SmartGates.

Voice recognition had previously been used by just six percent of respondents. Those living in a capital city were significantly more likely to have used this technology (7%, n=23) than those living elsewhere (1%, n=2) ($\chi^2(1, n=446)=3.83, p<0.05$).

Finally, when the results for the four biological biometric technologies (fingerprint, facial, iris and voice recognition) were combined, it was found that 25 percent (n=111) of respondents had previously used at least one of these biometrics, but no statistically significant differences were found between use of any form of biometric and the demographic characteristics examined.

Willingness to use security measures in the future

Respondents were also asked whether they would be willing to use these technologies in the future to protect personal information—for example, at ATMs, at airports, for computers, and for building access. Consistent with 2016, almost all respondents (94%) reported a willingness to use at least one of these technologies to protect personal information in the future (see Table 2; Goldsmid, Gannoni & Smith 2018).

The security measure respondents were most commonly willing to use in the future was passwords (79%), followed by fingerprint recognition (64%). The technology respondents were least willing to use in the future was a computer chip implanted under the skin (9%).

When 2016 and 2017 data were compared, there was a statistically significant 56 percentage point increase in the willingness to use passwords. There were modest increases in willingness to use voice recognition (5 percentage points), signatures (3 percentage points), facial recognition (3 percentage points) and iris recognition (3 percentage points; Goldsmid, Gannoni & Smith 2018).

Table 2: Willingness to use security measures to protect personal information in the future (%)

Survey year	2014	2016	2017	
Sample size (n)	5,000[a]	9,956	9,947	
Technology				**Percentage point change**
Passwords	73.5	22.2	78.6	+56.4***
Signatures[b]	–	43.6	46.5	+2.9***
Voice recognition	31.2	33.2	38.4	+5.2***
Fingerprint recognition	60.5	62.9	63.8	+0.9
Facial recognition	36.8	42.6	45.3	+2.7***
Iris recognition	40.8	39.6	42.3	+2.7***
Computer chip implanted under your skin[c]	–	–	9.4	–
Any technology[d]	95.7	93.8	94.3	+0.5
No technology	4.3	6.2	5.7	–0.5

***statistically significant at p<0.001

a: In 2014, only respondents who had experienced misuse of personal information in the preceding 12 months were asked about willingness to use security measures

b: The 2014 survey did not ask about signatures

c: Included in 2017 identity crime survey only

d: Includes passwords, signatures, voice recognition, fingerprint recognition, facial recognition, iris recognition, and computer chip implanted under the skin (except for 2014, which excluded signatures and chip implants)

Note: Respondents could select multiple responses. 2014 data weighted by location; 2016 and 2017 data weighted by age and gender

Source: Identity crime surveys 2014, 2016 & 2017 [AIC data file]

These results are surprising given that 88 percent of respondents indicated having used passwords in the past, yet only 74 percent were willing to use them in the future. It could be the case that respondents misinterpreted this question. Rather than reporting their willingness to use passwords and acceptance of the privacy and other risks involved, they may have indicated their dissatisfaction with the convenience and efficiency of using passwords. As a result, although more respondents reported actually using passwords, a smaller percentage were satisfied with using passwords and might have preferred another system for user authentication (Goldsmid, Gannoni & Smith 2018).

Demographics and willingness to use security measures

Further analysis showed there to be no relationship between demographic variables and willingness to use passwords in the future (Goldsmid, Gannoni & Smith 2018).

In the case of fingerprint recognition technology, 61 percent (n=270) reported being willing to use this in the future. Statistically significant differences were found between willingness to use fingerprint recognition and age groups, with older respondents being more willing to use this technology than younger respondents (χ^2(6, n=446)=53.08, p<0.001). Indeed, 73 percent (n=64) of 55–64 year olds and 78 percent (n=58) of those aged 65 years and over were willing to use fingerprint recognition. In contrast, only 30 percent (n=6) of 18–24 year olds and 34 percent (n=31) of 25–34 year olds were willing to use fingerprint recognition. These findings could be explained by the greater familiarity that older people have with fingerprint recognition systems (Biometrics Institute 2015), or it may be that older Australians are more concerned about computer security than younger users (ACCC 2018). The reduced willingness to use biometrics among younger people may be due to younger people feeling that fingerprint recognition systems may delay or otherwise impede their use of smartphones and tablets, or younger users might have a greater level of understanding of the risks of biometric technologies.

There was also a statistically significant association between willingness to use biometrics and language spoken at home (χ^2(1, n=446)=7.47, p<0.01). Those who spoke English at home were more willing to use fingerprint recognition in future (62%, n=260) than those who spoke another language at home (34%, n=10).

Four in 10 (41%) respondents were willing to use iris recognition in the future. As with fingerprint technology, there were statistically significant differences between age groups, with older respondents being more willing to use this technology than younger respondents (χ^2(1, n=446)=7.47, p<0.01). Indeed, 52 percent (n=46) of those aged 55–64 years were willing to use iris recognition, as were 54 percent (n=40) of those aged 65 years and over. In contrast, only 23 percent (n=21) of those aged 25–34 years were willing to use iris recognition technology.

Similar age-related differences were found for willingness to use facial recognition technology (χ^2(6, n=446)=41.20, p<0.001). Those aged 55–64 years (54%, n=47) and those aged 65 years and over (52%, n=38) were more likely to be willing to use facial recognition than those aged 18–24 years (14%, n=3), 25–34 years (23%, n=21), or 45–54 years (31%, n=29). Willingness to use facial recognition also varied by the extent of computer use (χ^2(6, n=442)=19.00, p<0.01). Those who used a computer for five hours or less each week were less willing to use facial recognition in future (16%, n=4) than those who used a computer for 26–30 hours per week (60%, n=35).

Around a third of respondents (31%) were willing to use voice recognition technology in future. As with fingerprint, iris and facial recognition, willingness to use voice recognition varied with age, with older respondents being more willing than younger respondents to use this technology (χ^2(6, n=446)=20.43, p<0.01). Those aged 55–64 years were more willing to use voice recognition in future (40%, n=35) than those aged 25–34 years (21%, n=19). Willingness to use voice recognition also varied with computer usage (χ^2(6, n=442)=18.58, p<0.01). Those who used a computer for five hours or less per week (14%, n=4), or for 11–15 hours per week (18%, n=11) were less willing to use voice recognition in future than those who used a computer for 26–30 hours per week (46%, n=26).

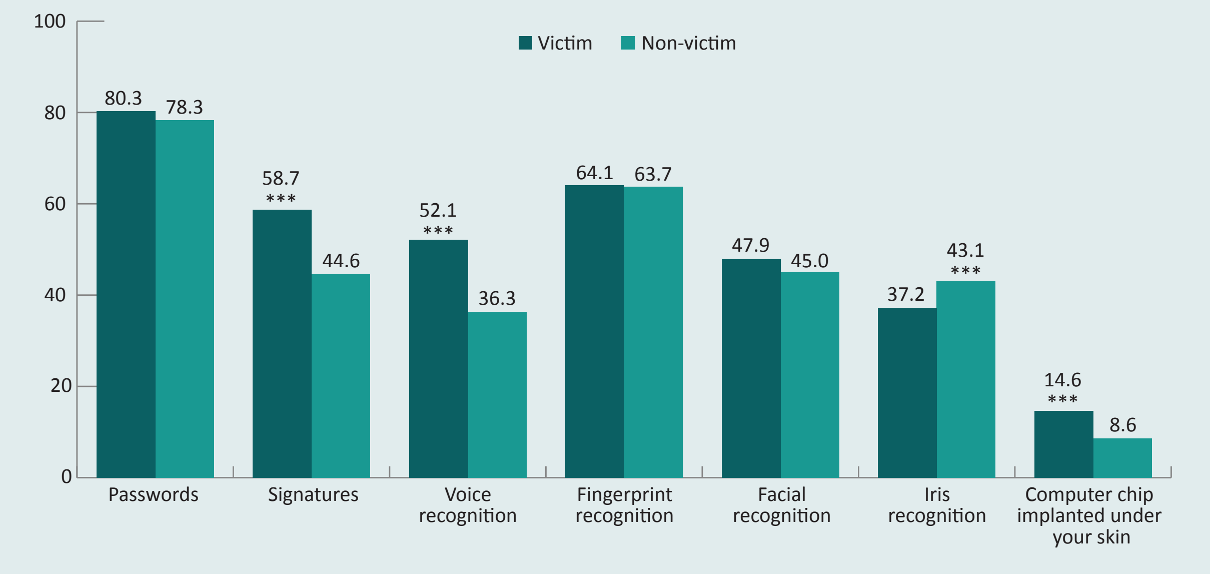
Again, when the results of the four biological biometric technologies (fingerprint, facial, iris and voice recognition) were combined, it was found that 68 percent (n=304) of respondents reported being willing to use at least one of these technologies in the future. As with prior use, there were statistically significant differences between age groups, with older respondents being more willing to use such technologies than younger respondents (χ^2(6, n=446)=39.31, *p*<0.001). Those aged 55–64 years (80%, n=70) and 65 years and over (85%, n=63) were more willing to use such technologies, while those aged 18–24 years (33%, n=7) and 25–34 years (45%, n=41) were less willing.

Finally, the analysis examined whether the willingness to use any of the four biological biometric technologies was affected by perceptions of whether the risk of personal information being misused in future would increase or decrease. No statistically significant differences were found, suggesting that willingness to use any of these four technologies was not influenced by perceptions of risk (Goldsmid, Gannoni & Smith 2018).

Victimisation and willingness to use security measures

Additional analysis of the 2017 survey findings was conducted to examine whether willingness to use security measures to protect personal information in the future was influenced by experiences of personal information misuse in the previous 12 months. Respondents who reported recent victimisation were significantly more likely than other respondents to report a willingness to use signatures (59% vs 45%; χ^2(1, n=9,947)=90.97, *p*<0.001, V=0.1), voice recognition (52% vs 36%; χ^2(1, n=9,947)=119.35, *p*<0.001, V=0.1) or a computer chip implanted under the skin (15% vs 9%; χ^2(1, n=9,947)=46.91, *p*<0.001, V=0.1; see Figure 3).

Figure 3: Willingness of victims and non-victims of misuse of personal information in the previous 12 months to use security measures to protect personal information, 2017 (%)



***statistically significant at *p*<0.001

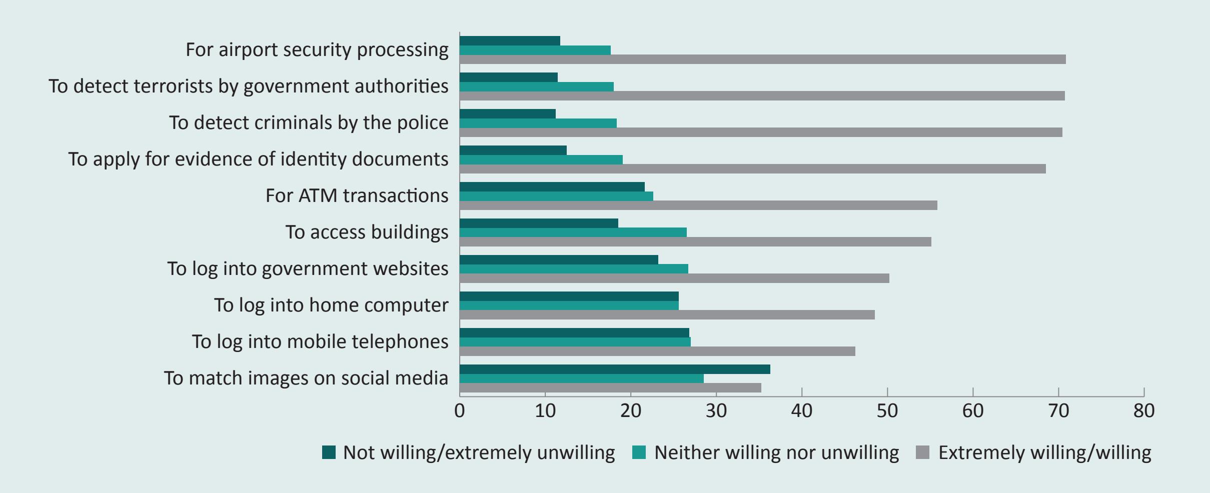
Note: Respondents could select multiple responses. Data weighted by age and gender; n=9,947

Source: Identity crime survey 2017 [AIC data file]

Willingness to use facial recognition for specific purposes

Further analysis was undertaken of the 2017 survey findings concerning willingness to use facial recognition technologies in various scenarios. Respondents were asked to respond to 11 facial recognition technology scenarios, using a five-point Likert scale ranging from extremely unwilling (1) to extremely willing (5). Figure 4 shows the results grouped into three categories—extremely willing/willing; neither willing nor unwilling; not willing/extremely unwilling.

Figure 4: Willingness of respondents to use facial recognition technologies for specific purposes, 2017 (%)



Note: Percentages may not total 100 due to rounding. Data weighted by age and gender; n=9,947

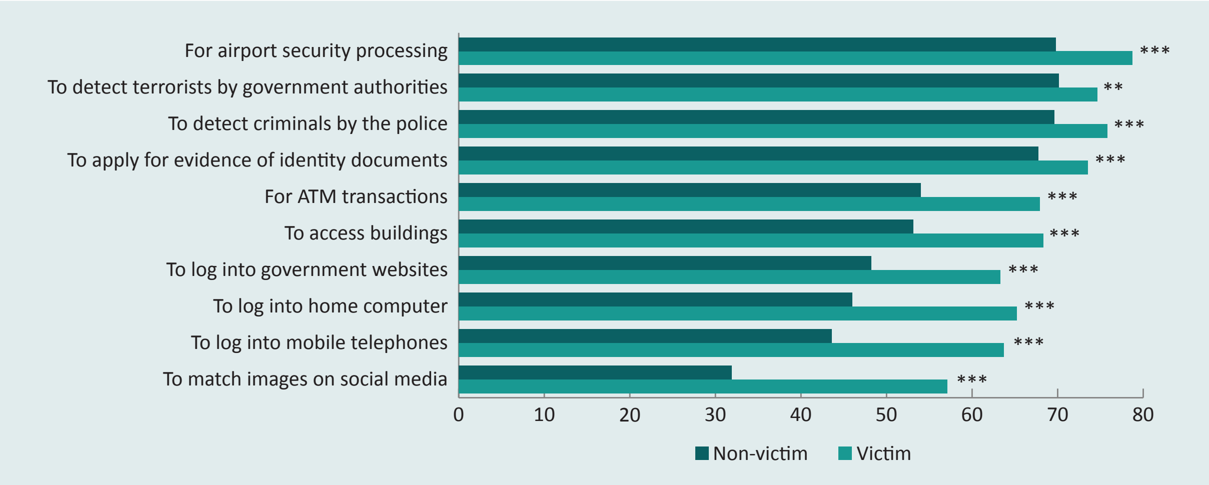
Source: Identity crime survey 2017 [AIC data file]

Respondents indicated that they would be most willing (ie willing & extremely willing responses combined) to use facial recognition technologies for government authorised purposes such as airport security, detection of terrorists or criminals or when applying for identity credentials. About half of respondents indicated they would be willing to use facial recognition technologies for ATM transactions, to obtain access to buildings, or to log on to mobile phones or government websites. Respondents were least willing to use facial recognition technologies for matching images on social media or logging onto computers at home. Apart from the use of facial recognition for logging onto government websites, there was less willingness to use the technology for private sector purposes than for official government purposes.

Comparing 2016 and 2017 data, there was a statistically significant 23 percentage point increase in willingness (ie willing & extremely willing responses combined) to use facial recognition for logging onto computers at home. There were modest increases of between six and two percentage points in willingness to use facial recognition for all other scenarios—the largest relating to mobile phones.

Figure 5 explores the difference between recent victims of personal information misuse and non-victims in their willingness to use facial recognition in various scenarios. Respondents who had been victims in the previous 12 months were significantly more likely than non-victims to report a willingness to use facial recognition for ATM transactions (68% vs 54%; $\chi^2(1, n=9,947)=89.94$, $p<0.001$, V=0.1), access to buildings (68% vs 53%; χ^2(1, n=9,947)=107.24, *p*<0.001, V=0.1), logging onto government websites (63% vs 48%; χ^2(1, n=9,947)=103.84, *p*<0.001, V=0.1), logging onto the home computer (65% vs 46%; χ^2(1, n=9,947)=168.06, *p*<0.001, V=0.1), logging onto mobile phones (64% vs 44%; χ^2(1, n=9,947)=185.18, *p*<0.001, V=0.1), and for matching images on social media (57% vs 32%; χ^2(1, n=9,947)=315.61, *p*<0.001, V=0.2).

Figure 5: Willingness[a] of victims and non-victims of misuse of personal information in the previous 12 months to use facial recognition technologies for specific purposes, 2017 (%)



***statistically significant at *p*<0.001, **statistically significant at *p*<0.01

a: 'willing' and 'extremely willing' responses combined

Note: Data weighted by age and gender; n=9,947

Source: Identity crime survey 2017 [AIC data file]

Conclusions

As the use of digital technologies has become more widespread, and identity crime and misuse have continued to increase, the computer security industry has sought to improve avenues for the efficient and secure authentication of users' identities. Existing systems that rely on username and password combinations have become problematic as criminals have become more adept at compromising passwords. The proliferation of username and password combinations has also made it impossible for users to manage this information without resorting to insecure ways of remembering their passwords, or having to purchase and use automated password management software (Emami, Brown & Smith 2016).

Biometric technologies seek to solve this problem by enabling individuals to use their biological attributes as a means of identifying themselves. This report presents the findings of recent surveys that sought to quantify the extent to which a sample of Australians have made use of different biometrics in the past, and how willing they would be to use the selected biometrics in the future to minimise the risk of criminal misuse of personal information.

With the rise of international security incidents, a balance must be struck between the need for personal security and the need for privacy and confidentiality of personal information. Prior research has found that concerns over privacy, data loss and spoofing (attempting to overcome biometric recognition systems) are important factors restraining the biometrics market. The present surveys confirmed that respondents were concerned about the privacy and confidentiality of personal information when using biometrics, particularly with systems operating outside government control. Understanding people's perceptions of risk and their willingness to use technology as a security solution is of critical importance in devising appropriate policy measures that will be effective on the one hand, and accepted by the community on the other (Emami, Brown & Smith 2016).

The current survey research showed that a relatively small percentage of respondents had used the specified biological biometrics in the past, but that use increased significantly between 2016 and 2017. It also showed that almost half (48%) of respondents in 2017 were willing to use one of the four biological biometrics to protect personal information in the future, and that this was a three percentage point increase on the same finding in 2016. Between 2016 and 2017 all the biometrics examined showed a statistically significant increase in user acceptance. In 2017, nine percent of respondents even reported being willing to use implanted chips to protect their personal information.

It was also found that older respondents were significantly more willing to use any of the four biological biometrics than younger respondents, perhaps indicating greater concern among older Australians regarding the security of their personal information, or perhaps their need to guard their assets and life savings from theft. Alternatively, younger people might be reluctant to use technologies that appear to be complex and could be seen to impede their immediate access to information in the online world. Clearly, ongoing monitoring of these attitudes is needed to ensure that future generations of users are willing to use any biometric systems that are implemented.

Respondents who reported recent victimisation were also significantly more likely than other respondents to report a willingness to use voice and iris recognition as well as chip implantation to protect their personal information, but not fingerprint or facial recognition systems.

As the biometrics market continues to develop, further research is needed to understand users' behaviour and willingness to use biometric technologies, particularly facial recognition and multi-modal systems that combine various biometrics, which are developing strongly. Evidence is needed of the extent to which such systems are vulnerable to fraud and misuse and how individuals respond to victimisation and reinstate their personal information following compromise. In addition, evidence is needed of the crime displacement effects of introducing biometrics and how criminal behaviour adapts and changes as a result of enhanced user authentication processes. In particular, risks of violent crime and duress inflicted on users need to be examined and strategies developed to address any such problems.

Acknowledgements

This study was undertaken as part of the Australian Government's National Identity Security Strategy. The survey was developed with input and advice from the Department of Home Affairs and the Attorney-General's Department. Data collection was undertaken professionally and efficiently by i-Link Research Solutions, a market research consultancy firm that provided a panel of individuals drawn from across Australia who were asked to complete an online questionnaire. The time and willingness of those who completed the survey are also gratefully acknowledged. The opinions expressed are those of the authors alone and do not necessarily reflect the views or policies of the Australian Government.

References

URLs correct as at November 2018

Attorney-General's Department (AGD) 2013. *National Identity Security Strategy 2012*. Canberra: AGD. Available from the Department of Home Affairs: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-security

Attorney-General's Department 2012. *A National Biometric Interoperability Framework for Government in Australia.* Canberra: AGD. Available from the Department of Home Affairs: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-security

Australian Competition and Consumer Commission (ACCC) 2018. *Targeting scams: Report of the ACCC on scams activity 2017.* Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2017

Biometrics Institute 2018. *Biometrics Institute industry trend tracker 2018.* Sydney: Biometrics Institute. Available online to members only: https://www.biometricsinstitute.org/resources/biometrics-institute-industry-trend-tracker-2018

Biometrics Institute 2015. Australian Federal Budget 2015 released: Good news for the biometrics industry but debate needed on the key issues. *Media release,* 14 May. https://www.biometricsinstitute.org/news/biometrics-institute-media-release-australian-federal-budget-2015-released.-good-news-for-the-biometrics-industry-but-debate-needed-on-the-key-issues

Department of Home Affairs 2018. Biometrics. Canberra: Department of Home Affairs. https://immi.homeaffairs.gov.au/help-support/meeting-our-requirements/biometrics

Department of Immigration and Border Protection (DIBP) 2017. *Annual report 2016–17.* Canberra: DIBP. https://www.homeaffairs.gov.au/reports-and-publications/reports/annual-reports

Emami C, Brown R & Smith RG 2016. Use and acceptance of biometric technologies among victims of identity crime and misuse in Australia. *Trends & issues in crime and criminal justice* no. 511. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi511

Goldsmid S, Gannoni A & Smith RG 2018. *Identity crime and misuse in Australia 2017: Results of the 2017 online survey.* Statistical Report no. 11. Canberra: Australian Institute of Criminology

Jorna P & Smith RG 2018. *Identity crime and misuse in Australia 2017.* Statistical Report no. 10. Canberra: Australian Institute of Criminology

Kim S 2015. ATMs that scan your eyeballs for cash being tested in U.S. *ABC News,* 26 Oct. http://abcnews.go.com/Business/atms-scan-eyeballs-cash-tested-us/story?id=34741159

Ma A 2018. Thousands of people in Sweden are embedding microchips under their skin to replace ID cards. *Business Insider,* 15 May. https://www.businessinsider.com.au/swedish-people-embed-microchips-under-skin-to-replace-id-cards-2018-5?r=us&ir=t

Planet Biometrics 2018. Australia's NAB and Microsoft develop biometric ATMs. *Planet Biometrics,* 23 Oct. http://www.planetbiometrics.com/article-details/i/8649/

Rowe E, Akman T, Smith RG & Tomison AM 2013. Organised crime and public sector corruption: A crime scripts analysis of tactical displacement risks. *Trends & issues in crime and criminal justice* no. 444. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi444

Saarinen J 2017. Mastercard trials fingerprint authentication for payments. *IT News,* 21 Apr. https://www.itnews.com.au/news/mastercard-trials-fingerprint-authentication-for-payments-459012?eid=1&edate=20170421&utm_source=20170421_AM&utm_medium=newsletter&utm_campaign=daily_newsletter

Smith M, Mann M & Urbas G 2018. *Biometrics, crime and security.* New York: Routledge

Smith RG 2007. Biometric solutions to identity-related cybercrime, in Jewkes Y (ed), *Crime online.* Cullompton: Willan Publishing: 44–59

Smith RG 2006. Identification systems: A risk assessment framework. *Trends & issues in crime and criminal justice* no. 324. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi324

Smith RG, Brown R and Harris-Hogan S 2015. *Identity crime and misuse in Australia: Results of the 2014 online survey.* Research and public policy series no. 130. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rpp/rpp130

Smith RG & Hutchings A 2014. *Identity crime and misuse in Australia: Results of the 2013 online survey.* Research and public policy series no. 128. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rpp/rpp128

Smith RG & Jorna P 2018. *Identity crime and misuse in Australia: Results of the 2016 online survey.* Statistical Report no. 6. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sr/sr6

Unisys 2014. *Unisys Security Index report Australia: Biometrics in airports.* https://www.unisys.com/ms/unisys-security-insights/australia/research-by-topic

United Kingdom Biometrics Working Group 2001. *Use of biometrics for identification and authentication: Advice on product selection.* https://www.idsysgroup.com/files/Biometrics Advice.pdf

United States Government Accountability Office (GAO) 2002. *Technology assessment: Using biometrics for border security.* GAO-03-174. Washington DC: GAO. https://www.gao.gov/products/GAO-03-174

Dr Russell G Smith is Principal Criminologist at the Australian Institute of Criminology and Professor in the College of Business, Government and Law at Flinders University.

Ms Alexandra Gannoni is a Senior Research Analyst at the Australian Institute of Criminology.

Dr Susan Goldsmid is a former Principal Research Analyst at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: aic.gov.au

ISSN 0817-8542

GPO Box 1936
Canberra ACT 2601, Australia
Tel: 02 6268 7166

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government